TOM DAVIS, VIRGINIA,
CHAIRMAN

DAN BURTON, INDIANA
CHRISTOPHER SHAYS, CONNECTICUT
ILEANA ROS-LEHTINEN, FLORIDA
JOHN M. McHUGH, NEW YORK
JOHN L. MICA, FLORIDA
MARK E. SOUDER, INDIANA
STEVEN C. LaTOURETTE, OHIO
DOUG OSE, CALIFORNIA
RON LEWIS, KENTUCKY
JO ANN DAVIS, VIRGINIA
TODD RUSSELL PLATTS, PENNSYLVANIA
CHRIS CANNON, UTAH
ADAM H. PUTNAM, FLORIDA
EDWARD L. SCHROCK, VIRGINIA
JOHN J. DUNCAN, JR., TENNESSEE
JOHN SULLIVAN, OKLAHOMA
NATHAN DEAL, GEORGIA
CANDICE MILLER, MICHIGAN
TIM MURPHY, PENNSYLVANIA
MICHAEL R. TURNER, OHIO
JOHN R. CARTER, TEXAS
WILLIAM J. JANKLOW, SOUTH DAKOTA
MARSHA BLACKBURN, TENNESSEE

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225–5074
FACSIMILE (202) 225–3974
MINORITY (202) 225–5051
TTY (202) 225–6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA,
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER,
MARYLAND
ELEANOR HOLMES NORTON,
DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE
CHRIS BELL, TEXAS

BERNARD SANDERS, VERMONT,
INDEPENDENT

"Developing Assurance on the Security of Software for the Federal Government"

Wednesday, September 17, 2003
10:00 a.m.

Room 2154 Rayburn House Office Building

Opening Statement of Chairman Adam Putman (R-Fl)

Good morning and welcome to another important hearing on cyber security. Today, the Subcommittee continues its aggressive examination of the information security issues most important to our Nation. As many of you know Secretary Ridge announced the creation of the U.S. Computer Emergency Response Team (US-CERT) in conjunction with Carnegie Mellon University.

This is an important step in the progress that needs to be made by our government in protecting the Nation's computers from cyber attack. It is no longer a question of if our computer networks will be attacked, but when, how often, and to what degree. Experts from the government and the private sector who have testified before this Subcommittee are very concerned that the United States is not adequately prepared to ward off a serious cyber attack that could cause severe economic devastation as well as potentially contribute to the loss of life.

Blaster and SoBigF are stark examples of how worm and virus vulnerabilities can cost us billions of dollars in lost productivity and administrative costs in a very short period of time. From the home user, to private enterprise, to the Federal government, we all need to take the cyber threat more seriously and move expeditiously to secure our Nation's computers. I look forward to continuing to work with DHS and other key federal agencies such as OMB, DOD, NIST, and NSA in this national security endeavor.

Today's hearing will examine the Common Criteria and whether or not a similar certification should be applied to all government software purchases. For years countries around the globe have wrestled with the inability to have a commonly recognized method of evaluating security software. Out of this climate the Common Criteria evolved and represents standards that are broadly useful within the international community

The international members of the Common Criteria share the following objectives:

1. to ensure that *evaluations* of *Information Technology (IT) products* and *protection profiles* are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
2. to improve the availability of evaluated, security-enhanced IT products and protection profiles;
3. to eliminate the burden of duplicating evaluations of IT products and protection profiles;
4. to continuously improve the efficiency and cost-effectiveness of the evaluation and *certification/validation** process for IT products and protection profiles.

The Common Criteria are maintained by an international coalition and is designed to be useful within the widely diverse international community. Currently, the Common Criteria Recognition Arrangement has 15 member countries. The National Security Agency and the National Institute for Standards and Technology represent the U.S.

Each member country accepts certificates issued by other members, making the Common Criteria a global standard. The criteria are technology neutral and are designed to be applied to a wide variety of technologies and levels of security.

The Criteria work by providing standardized language and definitions of IT security components. That standardization allows the consumer, in our case, the Department of Defense to create a customized set of requirements for the security of a product (called a protection profile). This profile would include the level of security assurance that the customer desires, including the various mechanisms that must be present for achieving that assurance. Alternatively, the Criteria allows the producer of the technology to develop their own set of targets (called a security target). An independent lab, overseen by the participating agencies (NIST and NSA in the U.S.) then tests the product against either the profile or the target and certifies that it can satisfy the requirements. Currently, the Department of Defense requires Common Criteria Certification for all security-related software purchases. NSA requires Common Criteria certification for all purchases for systems classified as national intelligence.

One of the more useful aspects of the Common Criteria is its ability to allow the purchaser of security software to compare "apples to apples." The protection profile, which is cast in the language of the Common Criteria, provides a view of security features independent of vendor claims. It allows a purchaser to find out, with certainty, the security features in a product, and to compare that product with other similar ones to determine which one to purchase.

The certification process, conducted by independent labs overseen by Common Criteria members (NIST in the U.S.), concentrates on analyzing the documentation provided by the vendor, testing the product, documenting its result and reporting out to its oversight agency. The oversight agency than reviews the validation report and issues a certification. The certification process is paid for by the vendor and can be both expensive and time consuming. Estimates for operating systems can be anywhere from 1-5 years and cost millions of dollars.

The expense and time commitment of the process has given rise to some questioning of the usefulness of the process. For example, the adoption of Common criteria could shut small vendors out of the acquisition process because they might not have the resources to go through certification. Another potential problem is timing. Because certification takes a significant amount of time, the government might not get the most cutting-edge technology available. Conversely, the government does need to gain assurance that security features in products exist and function as advertised.

This is the larger question that we are faced with: How can we – government-wide -- get the most secure products available in a timely and cost efficient manner and at the same time have IT companies compete on a level playing field in a competitive market that rewards and doesn't stifle innovation?

I look forward to the expert testimony we will hear today and thank the witnesses for their participation.

Today's hearing can be viewed live via WebCast by going to **http://reform.house.gov** and then clicking on the link under "Live Committee Broadcast".